Lokális vezetéknélküli technológiák

Az alábbi cikkünkben a lokális vezetéknélküli hálózatok építésére alkalmas technológiákat tekintjük át, ismertetjük főbb tulajdonságaikat, hogy az olvasó átfogó képpel rendelkezzen ezen a területen. Betekintünk a biztonság témakörébe, illetve felvázoljuk a technológia várható fejlődési irányát.

Számos vezetéknélküli technológia létezik már a piacon, melyeket az alacsony bitsebességtől az igen magas bitsebességig használnak helyhez kötött vagy mobil-, kereskedelmi vagy ipari alkalmazások során (pl. Bluetooth, 802.11 Wi-Fi és különböző magánhálózatok).

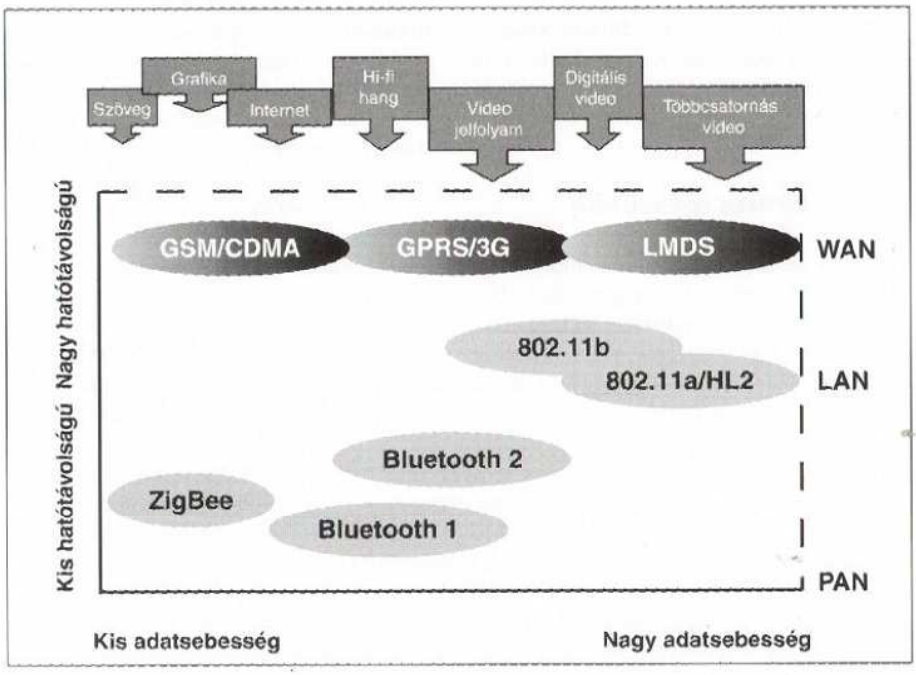
Az alábbi cikkben a vezetéknélküli lokális hálózatokban alkalmazott technológiák közül ismertetünk hármat.

WLAN

A WLAN (*Wireless Local Area Network*) egy kis hatótávolságú (30–150 m), vezetéknélküli, rádiós adatkommunikációs protokoll, amit elsősorban az irodai, vezetékes Ethernet-hálózatok leváltására terveztek. Segítségével különböző eszközök (kézi számítógépek, mobiltelefonok stb.) között lehet mobil-, IP-alapú, biztonságos kapcsolatot létrehozni. Jelenleg az alapötletből kiindulva több protokollt is kifejlesztettek, melyek egy részét az IEEE 802.11-es szabványcsaládja fog össze. Ebből következően az elérhető adatsebesség is különböző az alkalmazott megvalósításnak megfelelően (2, 5, 11, 54 Mbps).

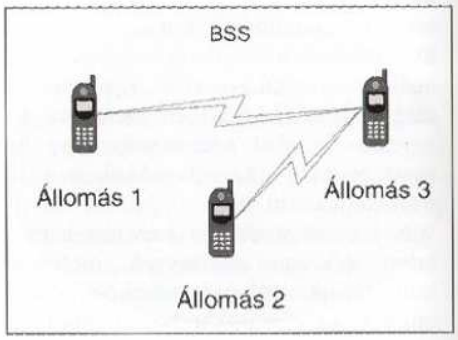
Az alábbiakban röviden, a WLAN működésének megértéséhez szükséges lényeget kiemelve ismertetjük a 802.11-es protokollcsaládra összességében jellemző főbb tulajdonságokat anélkül, hogy az alosztályok közötti különbségre kitérnénk.

1. ábra Vezetéknélküli hálózatok összehasonlítása



Hálózati topológia

A WLAN-hálózatok alkalmazhatóak a jelenlegi vezetékes hálózatok leváltására, illetve kiegészítésére is. Az általános hálózati topológiát a 2. ábrán láthatjuk. Itt a BSS (*Basic Service Set*) két vagy több vezetéknélküli állomást (STA, *Station*) tartalmaz, amik egymáshoz közvetlenül kapcsolódva szervezik saját magukat hálózattá, és biztosítják a lefedettséget a környezetükben. Két állomás között a kommunikáció közvetlenül vagy más, közbeiktatott állomásokon keresztül történik. Ezt a hálózati struktúrát *ad hoc* hálózatnak nevezzük, topológiája időszakos, az állomások helyzetétől és számától függően változhat.



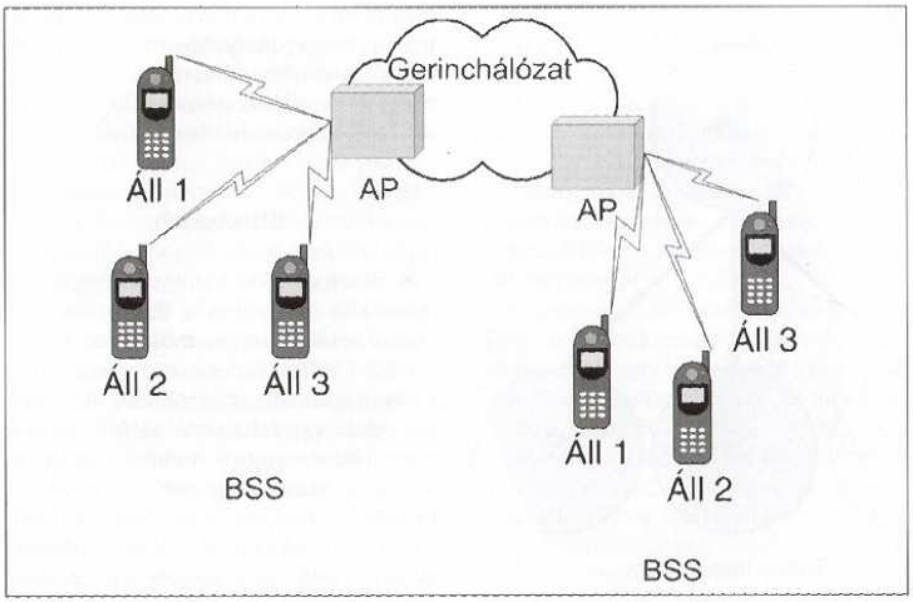
2. ábra Ad hoc hálózat

A BSS tartalmazhat egy speciális AP (*Access Point*) állomást is, melynek a feladata a vezetéknélküli és a vezetékes hálózatok közötti átjárás biztosítása (3. ábra). Ennek megfelelően rendelkezik mind vezetéknélküli, mind vezetékes illesztő felülettel.

Ha a BSS-ben egy AP is jelen van, akkor a BBS-ben lévő állomások egymás között nem, csak az AP-vel kommunikálnak, amin keresztül kapcsolatot teremthetnek egyfelől a saját BSS-ükben lévő szomszédjaikkal, illetve a gerinchálózat felhasználásával egyéb BSS-ek állomásaival, illetve a vezetékes hálózat számítógépeivel. Ezt a hálózati struktúrát infrastruktúra-hálózatnak nevezzük.

Rádiós technológia

A 802.11-es szabvány két fizikai hozzáférési módot határoz meg: a DSSS-t



3. ábra Infrastruktúra-hálózat

(*Direct Sequence Spread Spectrum*) és az FHSS-t (*Frequency Hopping Spread Spectrum*). A működési frekvenciatartomány a világszerte elfogadott a 2,5 GHz-es és 5 GHz-es ISM (*Industrial, Scientifical and Medical*) sávba esik, így a technológia könnyen bevezethető különböző országokban is.

A rádiós interfészen használt DSSS-kódolást már több rendszerben is alkalmazzák. A kódolandó adatfolyam bitjeit összeszorozzák hosszú PRSB (*Pseudo Random Binary Sequence*) szekvenciával (szórókóddal). Az így előálló nagy sebességű, széles sávszélességű jel kerül modulálásra a vivő frekvencián PSK (*Phase-shift keying*) modulációval.

Az így előállított jel védett a rádiós interfészen tapasztalható keskenysávú fading hatásoktól. A technológia alkalmas arra is, hogy a csatornán tapasztalható additív zajok hatását csökkentse, ugyanis a vételi oldalon történő jelvisszaállítás során a zavaró jel spektruma kiszélesedik, így egy sávszűrő alkalmazásával a vevő kimentén csökkenthető a zaj szintje. A szórókódok megfelelő megválasztásával (ortogonalitás) elérhető, hogy a közös rádiós csatornát használó adók a vételi oldalon megkülönböztethetőek legyenek, illetve a közeget egyszerre használó állomások száma ne legyen fixen korlátozott, számukat csak egy közelítő értékkel lehet maximálni.

Többszörös hozzáférés

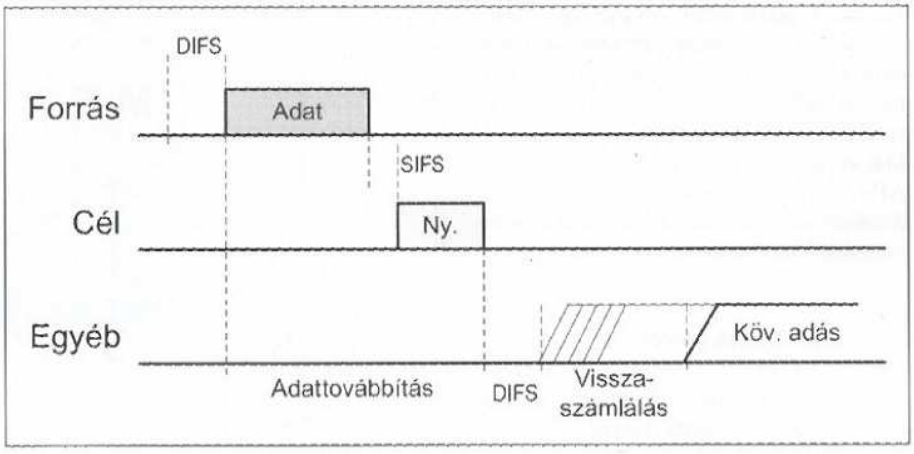
A 802.11 alap-hozzáférési eljárása a DCF (*Distributed Coordination Function*) kombinálva a CSMA-CA (*Carrier Sense Multiple Access / Collision Avoidance*) eljárással. Ennek során (4. ábra) az állomások figyelik egymás forgalmát. Ha egy állomás adni akar, akkor megnézi, hogy a csatorna egy bizonyos ideig (DIFS-idő, *DFC Interframe Space*) üres-e? Ha igen, elkezdi az adását, ha nem, akkor addig várakozik, amíg a csatorna üres nem lesz, és ekkor egy véletlen idejű várakozási visszaszámlálási állapotba kezd (*Backoff*). A visszaszámlálás végén ismét megkísérli a adást. Ennek az eljárásnak a segítségével megakadályozható, hogy egy adás befejeződése után az éppen várakozó állomások egyszerre kezdjenek meg adni, ütközést létrehozva a rádiós csatornán.

A kommunikáció során a vevő nyugtázza a vett csomagokat (ACKnowledgement). A rendszerben a helyes működés értelmében a nyugtázó csomagoknak elsőbbségük van, amit a SIFS (*Short Inert Frame Space*) idő DIFS-hez képesti lecsökkentésével érhető el.

A fent ismertetett eljárás feltételezi, hogy minden egyes állomás hallja a másik állomás adását. Ez azonban nem minden hálózati topológiában adott, így előfordulhat például olyan helyzet, amikor 3 állomás közül (A, B, C) csak az A-B és csak a B-C hallja egymást, az A-C nem. Ez a probléma „rejtett terminál" (*„Hidden node"*) néven ismert. Megoldásként egy másodlagos, virtuális vivőérzékelést iktattak a rendszerbe.

A 802.11-es hálózatokban az alapközeg-hozzáférési protokollon (DCF) kívül létezik egy PCF (*Point Coordination Function*) protokoll is, ami a DCF egy választható kiterjesztése. A PCF lehetőséget biztosít TDD (*time division duplexing*) csatornák használatára, melyek segítségével a WLAN alkalmas lesz a vonalkapcsolt, időben állandó szolgáltatások kiszolgálására, mint pl. a vezeték nélkülitelefon.

4. ábra CSMA-CA



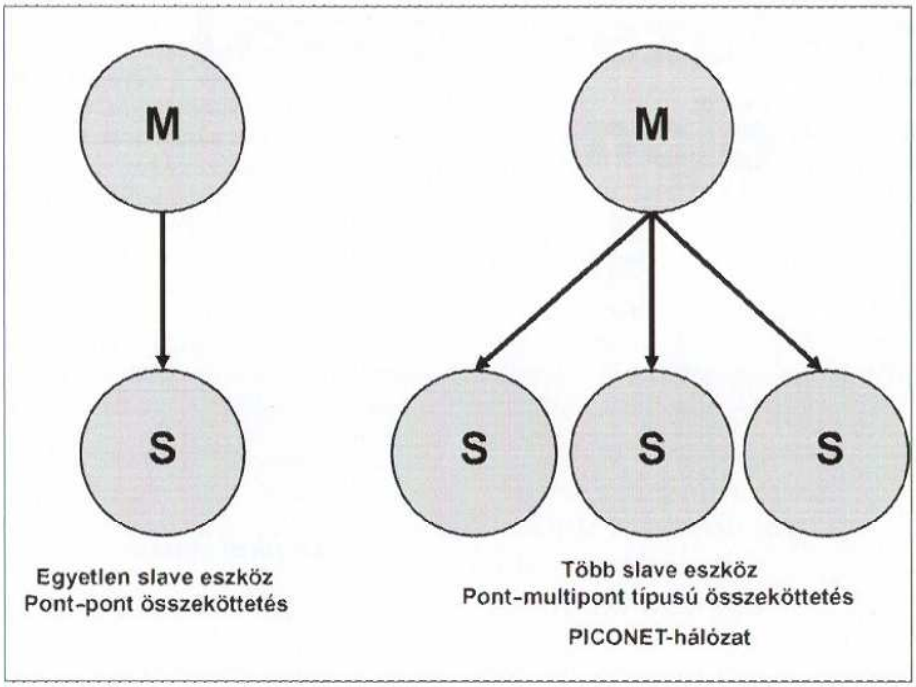
Logikai címzés

A 802.11-es szabvány megengedi, hogy a WLAN és az IEEE 802.3 Ethernet LAN infrastruktúra-hálózatokban átfogóan különböző címtartományokat használhassunk. A 802.11-es szabvány csak a vezetéknélküli kapcsolat címzését határozza meg, így az IEEE 802.11-es WLAN-ok integrálhatóak a LAN-okkal. Ennek megfelelően a címzésre az IEEE 802 48-bites címzési eljárását vették át az IEEE 802-es családdal való kompatibilitás megőrzése céljából.

Biztonság

A 802.11 két eljárással biztosítja a biztonságot: authentikációval és titkosítással. Az authentikáció során egy állomás ellenőrzi, hogy van-e jogosultsága kommunikálni egy másik állomással a lefedettség területen belül. Infrastruktúramódban az authentikáció az állomások és az Access point között történik. Az authentikáció lehet nyitott (*Open system*), vagy osztott kulcsú (*Shared key*).

A titkosítás meghatározásánál az volt a cél, hogy biztonsági szintje megközelít-



5. ábra Piconet-hálózat

se a vezetéknélküli hálózatok biztonsági szintjét. A WEP *(Wired Equivalent Privacy)* eljárás az RC4 PRNG algoritmusát használja az RSA-tól. A WEP-eljárás által biztosított kritériumok a következők:

- skálázható,
- önszinkronizáló,
- számításigény-hatékony,
- exportálható,
- választható.

Időzítés és energiagazdálkodás

Egy BSS állomásai között az órák időzítése periodikusan elküldött időbélyeget tartalmazó csomagokkal történik. Infrastruktúramódban a szinkronizáció referenciáját az AP biztosítja.

Az energiagazdaságosság igen fontos szerepet tölt be a kézi mobileszközökben, ugyanis itt a telep élettartama véges, így törekedni kell – a hosszú rendelkezésre állási idő miatt – a takarékosságra. Ennek megfelelően egy állomásnak két üzemmódja lehet: *„awake"* és *„doze"*. *„Awake"* üzemmódban az állomás teljes energiaellátású, csomag fogadására bármelyik pillanatban képes. *„Doze"* üzemmódban az állomásnak periodikusan „fel kell ébrednie", és meg kell kérdeznie az AP-t, hogy érkezett-e számára csomag. A *„doze"* üzemmódba lépés előtt az állomásnak értesítenie kell az AP-t.

A jövő

A WLAN fejlődése töretlen, a kezdeti szabványokat sorra dolgozzák át, és teszik alkalmassá a nagyobb sebességű adatátvitel használatára. Ezt elsősorban a hardverek számítási kapacitásának növekedése és az elmúlt években kibontakozó szoftverrádió-platform teszi lehetővé, illetve az, hogy a mobilpiac oly mértékű fejlődésen megy át, mely magával húzza – többek között – a WLAN technológiáját is. A WLAN piaci térhódítása töretlen, ma már nem csak az irodákban találkozhatunk vele, hanem reptereken, köztereken és szállodákban is készen áll arra, hogy kézi számítógépünk csatoló felületén vegyük igénybe és használjuk szolgáltatásait. Az eddigi gyakorlattal ellentétben, a WLAN-ok alkalmasak a nyílt, szolgáltatói hálózatok építésére, melyekben az interneteléréstől a multimédiás tartalomközvetítésén át a videókonferenciákig minden elérhető a felhasználó számára.

Bluetooth

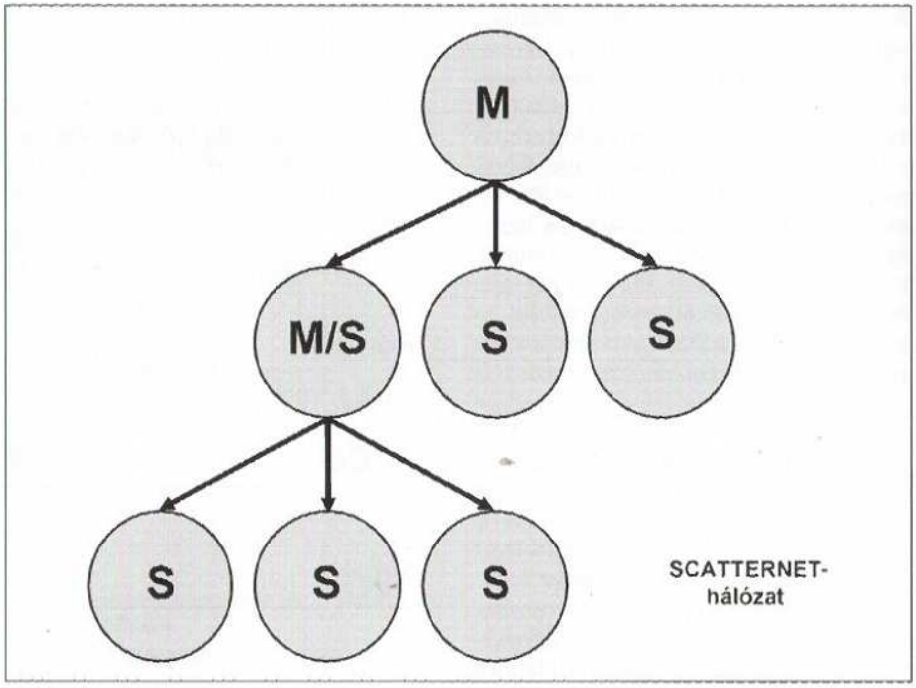
A Bluetooth kis hatótávolságú, vezetéknélküli szabványt a BSIG *(Bluetooth Special Interest Group)* dolgozta ki a rádiós SST-CDMA (kiterjesztett spektrumú technológia) megoldásokhoz, számítástechnikai vagy hasonló célú eszközök egymáshoz vagy mobilrádiótelefon-készülékekhez, vagy rajtuk keresztül a PLMN *(Public Land Mobile Network)* hálózathoz történő vezetéknélküli csatlakoztatása végett. A szabvány kidolgozása során figyelembe vették az IEEE 802.11 szabvány szerinti előírásokat is.

A Bluetooth-eszközök meghatározott felismerési, szinkronizálási, azonosítási és titkosító eljárások alkalmazásával építik fel az adott ad hoc vagy infrastrukturális helyi hálózatot. Az ilyen hálózatok állomásai, termináljai a saját hálózatukban, illetve a kapcsolódó hálózaton (GSM, UMTS, Internet) keresztül számos szolgáltatáshoz juthatnak hozzá.

Hálózati topológia

A különböző Bluetooth-eszközök többnyire egy kisebb ad hoc szerveződésű hálózatot alkotnak, és egyaránt képesek master vagy slave üzemmódban működni. Ráadásul a tervezés lehetővé teszi, hogy váltakozva legyen képesek

6. ábra Scatternet



az egyes üzemmódokra. A legegyszerűbb összeköttetés a pont-pont összeköttetés, ahol egy master egyetlen slave-vel van összekapcsolva. Abban az esetben, ha egy master-eszközhöz már több slave csatlakozik, akkor úgynevezett piconet-hálózatot alkotnak (5. ábra). Egyetlen master funkciót betöltő Bluetooth eszköz egyidejűleg 7 slave-eszközt képes kiszolgálni.

A harmadik lehetőség az, amikor az egyik piconetben szereplő slave-eszköz egy másik piconet-hálózatban master-funckiót tölt be, azaz összekapcsolja a két piconet-hálózatot. Az így kialakított hálózatot nevezik scatternet-hálózatnak (6. ábra). Ezáltal sokkal nagyobb lefedettségi területet lehet elérni, mint egy egyszerű piconet-hálózattal.

A master-eszköz feladatai közé tartozik a slave-eszközök között elérhető adatátviteli sávszélesség felügyelete, illetve kiszámolja a frekvenciaugratási szekvenciákat, és lefoglalja az adott kommunikációhoz a szükséges erőforrásokat. Emiatt a master lesz a felelős az időrések megfelelő kiosztásáért.

Rádiós technológia

A Bluetooth-eszközök a 2,4 GHz körüli ISM-sávban működnek (2400–2483,5 MHz). Sajnálatos módon ez a frekvenciasáv igencsak telített. A vezetéknélküli telefonok, garázsajtónyitók, a 802.11b szabvány és számos más alkalmazás is ezt a sávot használják. Emiatt a Bluetooth-eszközök az úgynevezett FHSS *(Frequency Hopping Spread Spectrum)* frekvenciaugratásos technikát alkalmazzák annak érdekében, hogy elkerüljék a többi eszközzel történő interferenciát.

A rendelkezésre álló frekvenciasávot a következő módon osztják fel: $f = 2402 + n$ MHz, ahol $n = 0...78$. A frekvenciaugrások mintegy 79 frekvenciát érintenek, amelyek szomszédos frekvencia értékei 1 MHz-es távolságra vannak egymástól.

A kommunikáció során másodpercenként 1600 frekvenciaugratást hajtanak végre, azaz egy időrés 625 µs-ra adódik. Természetesen ennek az időrésnek bizonyos részét (220 µs) egy biztonsági időrés tölti ki, melynek szinkronizáló szerepe van. Az adatok továbbítása pedig felváltva történik a master és a slave között (7. ábra).

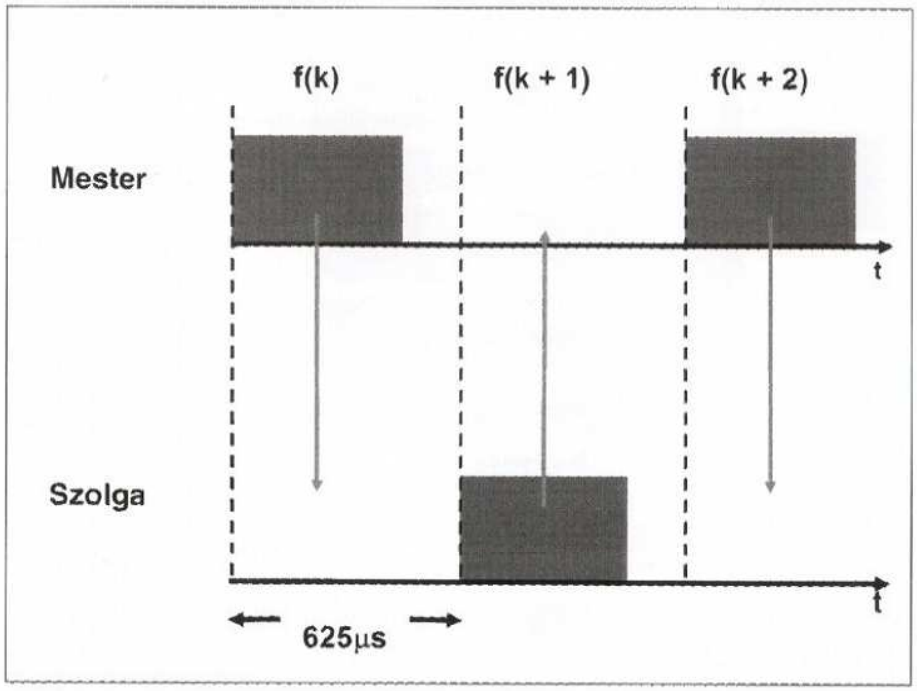
A Bluetooth kommunikációs csatorna alkalmas hang- és adatátvitelre is. Amennyiben szinkron hangátvitelre használjuk az összeköttetést, akkor 64 kbps érhető el a szinkron csatornán. Az aszinkron adatcsatornán a felfele irányban 57,6 kbps érhető el, lefele irányban pedig 721 kbps. Ellenben ha az adattovábbításra szinkron csatornát használunk, akkor mindkét irányban 432,6 kbps-t érhetünk el.

Többszörös hozzáférés

Több Bluetooth-egység összekapcsolásánál nincsenek olyan akadályok, mint a vezetékes környezetben levő eszközök hálózatba kapcsolásakor. Itt nem szükséges, hogy hasonló eszközök legyenek, hiszen a beépített kapcsolódási mechanizmusnak köszönhetően könnyedén felismerik a Bluetooth-technológiával felvértezett eszközöket.

Első lépésben a master megkeresi az összes elérhető Bluetooth-eszközt, majd a magukat láthatónak dedikált slave-eszközök egy FHS *(Frequency Hop Syncronization)* csomaggal válaszolnak, melyben szerepelnie kell az adott Bluetooth-eszköz címének és osztályának. A master begyűjti ezeket az FHS-csomagokat, majd az SDP *(Service Discovery Protocol)* segítségével egyeztet a slave-eszközökkel, hogy milyen típusú szolgáltatásokra lenne szükségük. Ezt követően page üzemmódra vált át, és elkezd kommunikálni az egyik kiválasztott eszközzel.

7. ábra Időrések kiosztása



Biztonság

A Bluetooth-hálózatban ugyanúgy jelen van az authentikáció és a titkosítási eljárás. Amennyiben megpróbáljuk összehasonlítani a Bluetooth biztonságát a WLAN hálózatokéval, akkor azt tapasztaljuk, hogy sokkal összetettebb, viszont egyidejűleg sokkal egyszerűbb is. Bonyolultabb abban az értelemben, hogy több biztonsági paramétert és beállítást tartalmaz, ellenben sokkal átláthatóbb, mert ezek a felhasználók számára transzparens módon jelennek meg. A Bluetooth biztonsága egy SAFER+ titkosítási algoritmuson alapul, mely eredetileg blokk-kódoló, de ebben az alkalmazásban folyamkódolóként működik. A Bluetoothnak három különböző biztonsági üzemmódja van:

- Mode 1: nem alkalmaz semmilyen authentikációs vagy titkosítási eljárást.
- Mode 2: csak a már kiépített kapcsolatban nyújt biztonságot.
- Mode 3: kapcsolat felépítése előtt kierőszakolja az azonosítást, és egyezteti a titkosítási eljárást.

A Bluetooth emellett külön nyújt biztonságot az eszközök és szolgáltatások számára. A szolgáltatások esetén is három különböző szintet lehet megkülönböztetni.

- 1. szint: nyitott minden felhasználó számára, nincs azonosítás és hozzáférés-ellenőrzés.
- 2. szint: van azonosítás, de hozzáférési engedélyt nem kell kérni.
- 3. szint: azonosítás és hozzáférési engedélyezés egyaránt szükségeltetik.

Első lépésben meghatározza egy adott eszköz megbízhatósági szintjét, majd egy úgynevezett PIN-kódot cserél a két kommunikálni kívánó Bluetooth-esz-

köz, melynek segítségével – és egy véletlenszerű számmal – egy 128 bites kulcsot generálnak és azt használják az authentikáció során. Miután ellenőrzik, hogy mindketten ugyanazt a kódot használják, az eszközök meghatároznak egy kölcsönösen elfogadott titkosítási kulcsot, melynek mérete 8 és 128 bit közötti lehet. A kapcsolat alatt végig ezt a kódot használják, és ha a későbbiekben is szeretnének adatot forgalmazni, akkor újra kell generálni ezt a kódot.

Időzítés és energiagazdálkodás

Mint minden alkalmazásnál, nagyon fontos a megfelelő időzítések alkalmazása. A Bluetooth esetében ez a gyakorlatban úgy néz ki, hogy egy új slave-eszköz felismerése tipikusan 3 s-nál hosszabb idő alatt következik be, hasonlóan egy alvó eszköz felébresztéséhez. Az aktív csatornához történő hozzáférés kb. 2 ms alatt történik meg. Annak ellenére, hogy egy eszköz hálózatba történő konfigurálása viszonylag hosszabb időt vesz igénybe, a Bluetooth tervezői többnyire arra fektették a hangsúlyt, hogy minél jobban megfeleljen az ad hoc hálózat igényeinek. Ennek az lett a következménye, hogy a telepfelvétel optimalizálását igencsak figyelmen kívül hagyták, és talán ez lett az egyik nagy hátránya a Bluetooth-eszközöknek, hiszen folyamatos használat mellett szinte 1-2 naponta feltöltésre van szükség. Energiafelhasználás szempontjából az eszközöket három kategóriára lehet osztani:

- Class 1: 100 mW (20 dBm) kimeneti teljesítmény, közel 100 m-es hatótávolság.
- Class 2: 2,5 mW (4 dBm) kimeneti teljesítmény, kb. 20 m-es hatósugár.
- Class 3: 1 mW-os (0 dBm) kimeneti teljesítmény, melynek hatótávolsága max. 10 m.

A 2-es és 3-as osztályokba tartozó eszközök adaptív teljesítményszabályozásra is alkalmasak. Ennek segítségével mérlegelik, hogy egy adott típusú összeköttetéshez mekkora energia szükségeltetik, ezáltal kímélik a telepet, illetve képesek csökkenteni a szomszédos interferenciák kialakulását.

A jövő

A Bluetooth-t arra tervezték, hogy személyközeli WPAN-hálózatot lehessen vele létrehozni, illetve több Bluetooth-egységgel ellátott számítástechnikai vagy mobileszközt összekapcsoljanak. A kezdeti problémákat áthidalva a Bluetooth 1.1-es változata már sokkal stabilabb volt elődjénél, viszont az igazi áttörést az 1.2-es változat 2004 év első harmadában történő bevezetése okozta. A javított felderítő képességének köszönhetően jelentősen felgyorsult az új eszközök felismerésének képessége (10–20 ms-ról lecsökkent kb. 5 ms-ra), viszont a korábbi eszközökkel való kompatibilitás érdekében az új eszközök többsége továbbra is kb. 10 ms alatt fejezi be a keresést. A javított protokoll rendszerének köszönhetően például sokkal jobb minőségben lehet továbbítani a hanganyagokat, illetve növelni lehet a telepek élettartamát, ami a Bluetooth-eszközök egyik kritikus problémáját okozza. Ráadásul csökkenni fog a szomszédos interferencia kialakulásának lehetősége, illetve a hibás adatátvitelek száma is drasztikusan csökkenni fog. Amennyiben a tendenciát nézzük, a Bluetooth-egységek egyre inkább alkalmazkodnak a mobiltelefónia igényeihez, ezzel is jelezve a különböző mobiltechnológiák jövőbeni konvergenciáját.

ZigBee

A Bluetooth-technológia remekül megállja helyét a beszédátviteli és a nagyobb adatátviteli sebességet igénylő alkalmazásokban, ellenben a ZigBee-technológia sokkal alkalmasabb az olyan felügyeleti alkalmazásokra, melyekhez nem kell nagyobb átviteli sebesség, viszont sokkal fontosabb a hatékony telepkihasználás, változtatható topológia, és csak kis mértékű felhasználói beavatkozás (pl. távirányítás) szükségeltetik. Nagyon fontos megjegyezni, hogy a hihetetlenül alacsony telepigény a kulcsa a ZigBee-szabványnak, hiszen ezzel lehetőség adódik hosszú élettartamú – nem újratölthető – elemmel működtethető eszközök alkalmazására is.

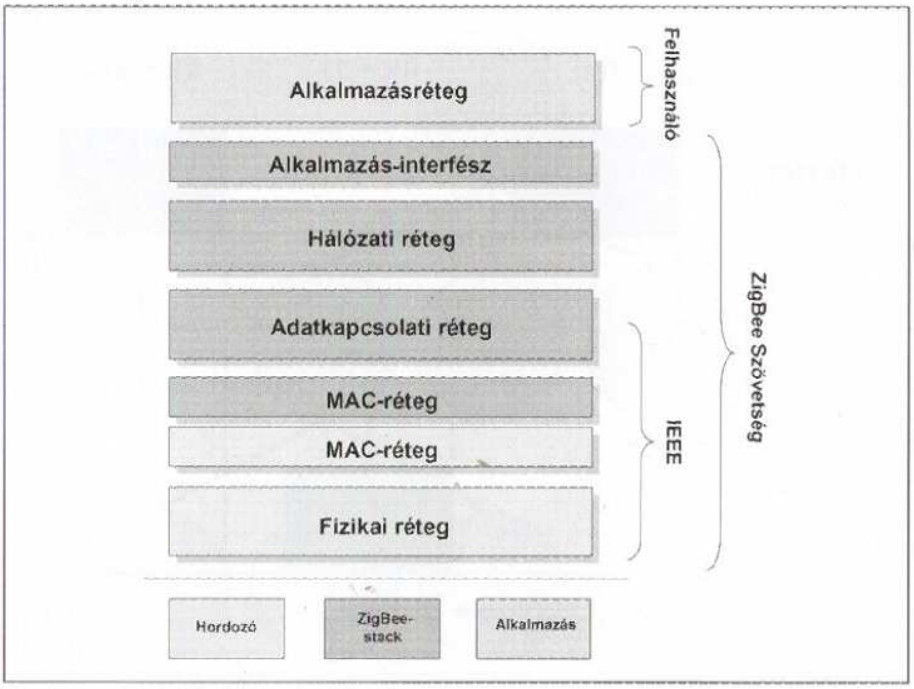
Az új ZigBee-protokoll tulajdonképpen egy nyílt szabványt jelent az alacsony teljesítményű vezetéknélküli hálózatokban a különböző eszközök megfigyelésére és felügyeletére. Az IEEE 802.15.4 szabvánnyal együttműködve – mely az alacsony átviteli sebességű PAN-okra (*Personal Area Network*, személyközeli hálózat) összpontosít, és egyben definiálja az alacsonyabb szintű protokollszinteket (pl. fizikai réteg: PHY; közeghozzáférési réteg: MAC) – a ZigBee a protokoll-stack magasabb rétegeit definiálja a hálózati rétegtől az applikációs rétegig, beleértve az alkalmazásprofilokat is. A ZigBee ennek megfelelően az ISM-sávot használja működése során, ezzel is biztosítva azt, hogy a földrajzi helytől függetlenül is lehessen alkalmazni.

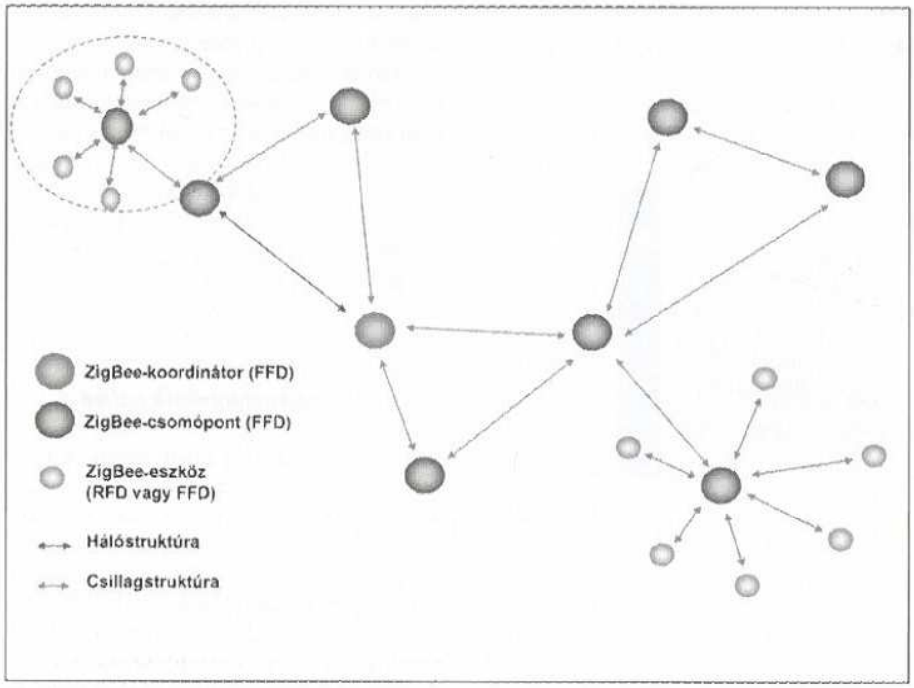
A ZigBee és az alatta elhelyezkedő 802.15.4 szabvány a rendszertervezők számára eltérő működési osztályú készülékek alkalmazását biztosítja:

- csökkentett képességgel rendelkező eszközök (RFD, *reduced functionality device*),
- teljes működési képességgel rendelkező ezsközök (FFD, *full functionality device*),
- hálózat felügyeleti eszköz (*network coordinator*).

Minden egyes ZigBee-hálózat rendelkezik legalább egy RFD-vel vagy FFD-vel, illetve egy hálózat koordinátor-

8. ábra ZigBee-protokoll-stack





9. ábra Hálózati topológia

ral. Az érzékelős alkalmazások többsége eredendően RFD-osztályba esik, a kiterjesztett hálózatokban pedig az FFD-ket, illetve a hálózati koordinátorokat arra késztetik, hogy áthidalják és összeköttetéseket teremtsenek ott, ahol a hálózati topológia szükségessé teszi.

Hálózati topológia

Az egyik leggyakoribb hálózati topológia a csillagstruktúra, melyet széles körben alkalmaznak a különböző hálózati felépítésekben. Nagyobb kiterjedésű környezetben már sokkal inkább használják a fatopológiát, mely alkalmas több csillagtopológiájú hálózati részt egyesíteni.

A ZigBee-alkalmazások többsége viszont a hálóstruktúra használatát részesíti előnyben, ugyanis sokkal rugalmasabb útvonalválasztást tesz lehetővé, illetve az egyes csomópontok mozgásából vagy pillanatnyi kieséséből eredő hibákat könnyebben ki lehet küszöbölni. A hálózati koordinátor feladatai:

- a hálózat folyamatos szervezése,
- beacon-üzenetek továbbítása,
- különböző hálózati csomópontok menedzselése,
- az összepárosított eszközök közötti üzenetek irányítása.

A hálózati csomópontok feladatai:

- teleppel működnek és energiatakarékosságra törekednek,
- elérhető hálózatok figyelése,
- a hozzájuk kapcsolódó eszköztől továbbítják a hálózatba az üzenetet,
- eldöntik, hogy a beérkezett adat melyik eszközhöz továbbítandó,
- hosszabb idejű alvó állapot.

A ZigBee-hálózatban a hálózati koordinátorok és a hálózati csomópontok (routerek) funkcionalitásuk szempontjából az FFD működési osztályba tartoznak.

Rádiós technológia

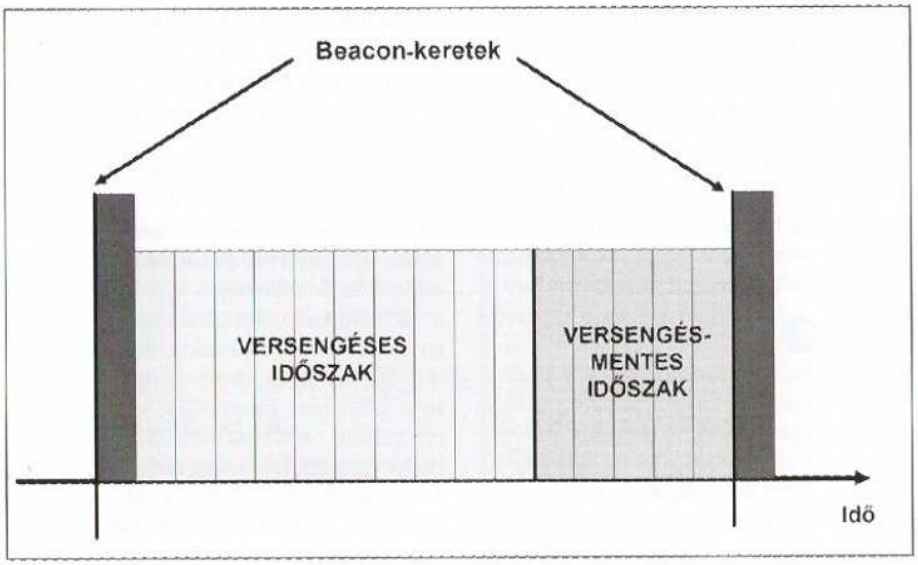
A ZigBee-alkalmazásokban az adatok megbízható továbbítása nagyon fontos feladat. Az alatta levő 802.15.4 szabvány a különböző szintek között meglehetősen nagy biztonságú adatátvitelt biztosít. Példának okáért 27 átviteli csatornát alkalmaz az összesen három elkülönülő frekvenciatartományban.

Ahogy a 10. ábrán is látható, a 2,4 GHz-es tartományt világszerte alkalmazzák. Ebben a sávban 16 db olyan csatornával rendelkezik, melyek adatátviteli sebessége egyenként eléri a 250 kbps-t. Természetesen alacsonyabb frekvenciasávokat is definiál. A 902–928 MHz-es tartományt többnyire a USA-ban használják, ebben 10 db egyenként 40 kbps átviteli sebességű csatorna található. Az európai alkalmazások során használni lehet még egy csatornát 868 MHz-en, mely 20 kbps sebességet biztosít a felhasználóknak. A frekvenciák eme bőséges kínálata lehetőséget nyújt az alkalmazások számára, hogy az adott hardveres konfiguráció mellett valós időben alkalmazkodjanak a lokális interferencia- és/vagy a terjedési viszonyokhoz.

A 802.15.4-es szabványban a fizikai rétegben több modulációs eljárást alkalmaznak. A 868–915 MHz-es frekvenciasávokban BPSK *(Binary Phase Shift Keying)* modulációt használnak, ellenben a 2,4 GHz körüli ISM-sávban már az O-QPSK *(Offset Quadrature Phase Shift Keying)* modulációt helyezik előtérbe. Mindkét modulációs eljárás kiválóan alkalmazható alacsony jel-zaj viszonyú környezetben. Fizikai hozzáférés szempontjából a ZigBee-alkalmazásokban a DSSS-t használják, ami önmagában már egyfajta többbutas teljesítmény- és vevőérzékenység-javulást hordoz a jelfeldolgozási erősítésén keresztül.

10. ábra Frekvencia kiosztása

	FREKVENCIA-SÁV	LEFEDETTSÉG	ADATSEBESSÉG	CSATORNÁK SORSZÁMA
2,4 GHz	ISM	Világszerte	250 kbps	11–26
868 MHz		Európa	20 kbps	0
915 MHz	ISM	Amerika	40 kbps	1–10



11. ábra Versengéses és versengésmentes időszakok

A keretszerkezetet úgy tervezték meg, hogy annak bonyolultságát igyekeztek minimalizálni, ugyanakkor a zajos csatornában is képes legyen továbbítani az adatokat. Az IEEE 802.15.4 MAC-rétegben négy különböző keretszerkezetet definiáltak: beacon, adat, nyugta és MAC-felügyelet.

Minden egyes adatcsomag megérkezése után a vevő egy 16 bites CRC-ellenőrzést hajt végre, és ennek függvényében küld nyugtát az adónak a sikeres kézbesítés megtörténtéről. Amennyiben hibát észlel, a beérkezett csomagot eldobja, és nem küld nyugtát. Természetesen lehet úgy is méretezni a rendszert, hogy ha nem érkezik bizonyos időn belül nyugta a sikeres vételről, akkor néhányszor újra küldi az adott csomagot ezzel próbálva biztosítani a sikeres kézbesítést. Amennyiben az adó és vevő között a rádiós összeköttetés kevésbé megbízható, vagy valamilyen hálózati hiba lép fel, akkor a ZigBee, ha lehetősége van rá, az önjavító képességének köszönhetően alternatív útvonalat próbál meg keresni két állomás között.

Többszörös hozzáférés

A LR-WPAN *(Low Range – Wireless Personal Area Network)* hálózatban lehetőség van úgynevezett szuperkeret-struktúra használatára is a többszörös hozzáférés által okozható problémák elkerülésére. A szuperkeretet a hálózati koordinátor küldi ki a hálózatba és 16 egyenlő időrést tartalmaz. A beacon-üzenetet mindig egy ilyen szuperkeret elején küldi ki, melynek szerepe a kapcsolatban levő eszközök szinkronizálása, a PAN azonosítása és a szuperkeret szerkezetének leírása. Az üzenni kívánó eszközök a versengéses időszakban (CAP, *Contention Access Period)* a CSMA-CA szabályainak megfelelően tudnak kommunikálni. A PAN-koordinátor bizonyos eszközöknek, illetve alkalmazásoknak lefoglalhat fix időréseket (GTS, *Guaranteed Time Slot)*, melyek az adott szuperkeret végén jelennek meg.

Emiatt a versengéses időszakban a kommunikálni kívánó feleknek azt is figyelembe kell venniük, hogy a még a versengésmentes időszak (CFP, *Contention Free Period)* előtt be tudják fejezni az adási szándékukat. Illetve a CFP-ben adó eszközöknek biztosítaniuk kell, hogy a nekik kirendelt időrésekben vagy legkésőbb a szuperkeret versengésmentes időszakának végéig befejezik az adásukat.

Biztonság

Az érzékelős alkalmazásoknál nagyon fontos az adatátvitel során a megfelelő biztonság kialakítása, hiszen nem célszerű, ha más eszközök képesek értelmezni vagy befolyásolni azok tartalmát. Az IEEE 802.15.4 szabványban definiálva vannak az authentikációs folyamatok, illetve a titkosítási szintek, ahol a fejlesztők kiválaszthatják, milyen fokú titkosítást szeretnének alkalmazni a kommunikáció során. Ellenben nem tudja garantálni a titkos kulcsok hálózaton történő továbbítását, mely a ZigBee feladata lesz.

A ZigBee biztonsági eszköztára tartalmaz olyan elemeket, melyek segítségével biztonságosan lehet távolról is felügyelni a rendszer működését. Azon alkalmazásokban, ahol az adatbiztonság kevésbé kritikus (pl. hőmérő-alkalmazás), a rendszer tervezői eldönthetik, hogy mennyire biztonságossá tegyék a rendszert. Ennek oka az, hogy kevesebb biztonsági képesség implementálásával javítani lehet a telepek élettartamán és csökkenteni lehet a bekerülési költséget. Ellenben ipari vagy katonai alkalmazások esetén, ahol nagyon fontos az adatok sértetlensége, ott a biztonsági paraméterek garanciája prioritást élvez.

Időzítés és energiagazdálkodás

A ZigBee-alkalmazások egyik kulcsfontosságú része a hatékony időzítések alkalmazása. Egy újabb slave-eszköz besorolása kb. 30 ms-ot vesz igénybe, az alvóból az aktív állapotba történő váltása tipikusan 15 ms alatt történik, illetve az aktív slave-csatorna hozzáférési ideje is 15 ms. Elmondhatjuk, hogy a ZigBee-eszközök nagyon hamar tudnak csatlakozni, adatokat továbbítani, lekapcsolódni, illetve gyorsan tudnak alvó állapotba kerülni. Ezáltal biztosítják a telepek kapacitásának kímélését. Ha ezt összehasonlítjuk a Bluetooth-eszközök működésével, akkor azt tapasztaljuk, hogy azok hozzávetőlegesen 100-szoros energiát igényelnek ugyanazon műveletek végrehajtásához. A ZigBee-eszközöket úgy tervezték, hogy optimalizálják a telepfelvételt, ezáltal akár egyetlen átlagos ceruzaelemmel is több mint 2-3 évet képesek működni egyhuzamban.

A jövő

Összességében elmondható, hogy a ZigBee és az alatta levő 802.15.4 kommunikációs technológia alaposan meg fogja változtatni a közeljövő vezetéknélküli technológiáját, különösen a vezetéknélküli érzékelők megjelenésével, melyek működéséhez megbízható adatátvitelt garantál, hosszabb telephasználati üzemidőt biztosít, illetve alacsonyabb telepítési és üzemeltetési költséggel fog tudni működni. Az IEEE 802.15.4 gyakorlatilag már készen áll a bevetésre, a ZigBee hálózati, biztonsági és profilspecifikációinak véglegesítése 2004 közepére tehető. Az első, piacon is megjelenő termék a 2004-es év vége fele várható. A ZigBee Alliance tagsága minden ipari érdeklődő és befektető számára nyitott szervezet.

A lokális vezetéknélküli technológiák fejlődése

Ismertettük a ma elérhető, vezetéknélküli lokális hálózatok építésére alkal-

mazható technológiákat. Fejlődésük töretlen, sebességben és szolgáltatásokban napról napra többet nyújtanak, azonban ha figyelemmel kísérjük az egyéb, jelenleg még nem lokális hálózatok építésére tervezett rádiós technológiákat, mint a GPRS *(General Packet Radio Service)*, az EDGE *(Enhanced Data rate for GSM Evolution)*, a 3G és társai, akkor azt tapasztalhatjuk, hogy rohamos fejlődésükkel egyre inkább behozzák mind sebességbeli és mind költségbeli hátrányukat. A tendenciákból következtethető, hogy a jövőben a lokális hálózatok, mint szuverén egységekként történő általános és széleskörű alkalmazásuk egyre ritkább lesz, az új, gyors és közvetlen internetkapcsolatot biztosító hozzáférések egyre jobban ki fogják szorítani őket. A VPN *(Virtual Private Network)* alkalmazásával már határok nélküli zárt hálózatokat alkothatunk, így elképzelhető, hogy a jövő lokális hálózata már nem lesz a szó szoros értelmében vett lokális hálózat, hanem sokkal inkább az internet közegén egy virtuális hálózat.

Butyka Zsolt–Jursonovics Tamás

Irodalom

(1) ANSI/IEEE Std 802.11, 1999 Edition www.ieee.org
(2) www.wi-fi.org
(3) Bluetooth SIG, http://www.bluetooth.org
(4) Understanding Bluetooth, Jan. 2002. HP-invent
(5) Matt Ziegler: An Overview of Bluetooth: Architecture, Power Consumption and Performance, CSE End of Term Report
(6) ZigBee Alliance, http://www.zigbee.org
(7) Jon Adams: Meet the ZigBee Standard, ZigBee Alliance
(8) Patrick Kinney: ZigBee Technology: Wireless Control that Simply Works, Communication Design Conference, 2. October 2003.